MAINGATE

User Guide

IP Connect GPRS

Wireless Maingate

Document number: MG040123 PdM F
Date: 2007-10-03
Information class: Open Information

Address: Wireless Maingate
Box 244
S-371 24 KARLSKRONA
Sweden

Phone number: +46 455 36 37 00
Fax number: +46 455 36 37 37

© Copyright Wireless Maingate Nordic AB 2007

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing.
Wireless Maingate Nordic AB shall have no liability for any error or damages of any kind resulting from use of this document.

TABLE OF CONTENTS

1	INTRODUCTION	4
2	PRODUCT OVERVIEW	5
3	ORDERING IP CONNECT	6
4	DEVICE IP RANGES	8
5	IP CONFIGURATION	9
6	REGISTERING TERMINALS	11
7	COMMUNICATION	13
8	SECURITY ASPECTS	15
9	INVOICING	17
10	SUPPORT	18
11	REFERENCES	19
12	DOCUMENT HISTORY	19

1 INTRODUCTION

This document is intended to be used by the customer during ordering, configuration and use of the Wireless Maingate IP Connect GPRS product.

1.1 TERMINOLOGY

Account	An IP Connect GPRS account containing a group of terminals and a customer application between which communication can take place
API	Application Programming Interface
APN	Access Point Name
CSD	Circuit-Switched Data
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
IP Default Route	Default destination of unspecified IP packets
LAN	Local Area Network
NTP	Network Time Protocol
PDP	Packet Data Protocol
PPP	Point-to-Point Protocol
RADIUS	Remote Access Dial-in User Service
TCP/IP	Transmission Control Protocol/Internet Protocol
VPN	Virtual Private Network
XML	Extensible Mark-up Language

© Copyright Wireless Maingate Nordic AB 2007

2 PRODUCT OVERVIEW

IP Connect GPRS provides transparent IP communication between a customer application and terminals equipped with GSM/GPRS modems using fixed IP addressing. An overview of the functionality is shown in Figure 1.

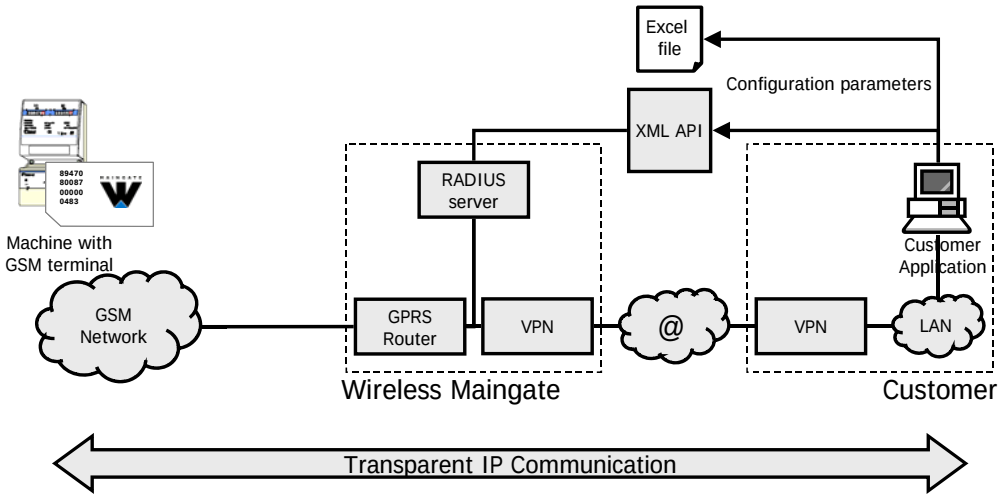


Figure 1 – Product overview

The customer application is connected to Wireless Maingate over Internet using a VPN tunnel. Each terminal is configured once in Maingate's RADIUS with desired parameters that control the communication settings, through an XML API or Excel file. Once the configuration has been done, communication is initiated by activating a GPRS PDP Context and thereafter sending IP packets from application or from a terminal.

The VPN tunnel could either be set up "site-to-site", as in figure above, or directly from a host with VPN client software provided by Maingate.

2.1 PRODUCT SPECIFICATIONS

The IP Connect GPRS product supports the following functionality:

- Support for IP addressing according to IP v4

2.2 TERMINAL REQUIREMENTS

In order for the IP Connect GPRS product to be successfully used with a terminal, the terminal must satisfy the following requirements:

- The terminal must be equipped with a GSM modem that supports GPRS
- The terminal must be equipped with a Maingate GSM subscription
- The terminal must support PPP according to RFC 1661 of the IETF
- The terminal must support dynamic IP address allocation over PPP
- The terminal must use Default Route or alternatively static routing must be defined for IP Connect GPRS.

© Copyright Wireless Maingate Nordic AB 2007

3 ORDERING IP CONNECT

The IP Connect GPRS product is ordered by filling in and signing the Product Agreement. The signed agreement can be delivered in original to a Maingate sales representative or sent by post to Maingate. The pages of the Product Agreement are shown in Figure 2.

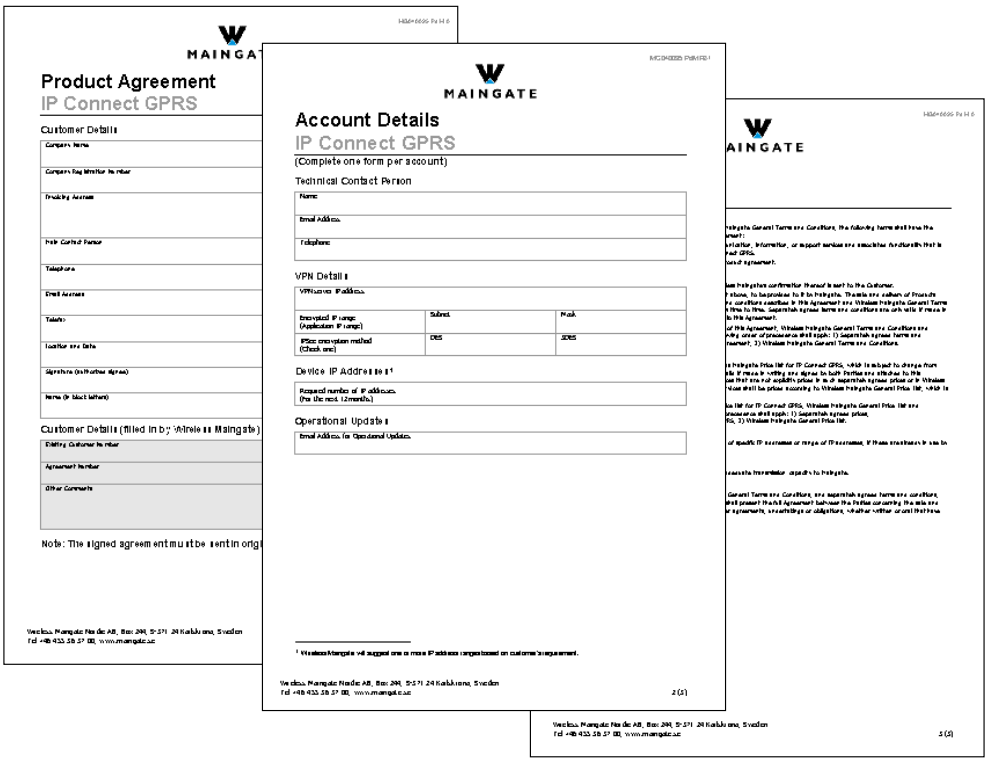


Figure 2 – IP Connect GPRS Product Agreement

One separate form for Account Details (page 2) is required for each separate account that is required. The Account Details are filled in as follows:

Technical Contact Person	Contact details of the person responsible for configuring the VPN tunnel at the customer.
Operational Updates	Email address of customer representative that shall receive updates concerning operational issues, such as planned or unscheduled outages, from Maingate.
VPN Configuration	VPN configuration, either LAN to LAN or VPN Client
Requested IP Size	An estimate of the number of IP addresses that are required for the account. One IP address is required for each terminal that shall use IP Connect GPRS. Based on the required number, Maingate will suggest a suitable range to the customer.

NOTE! Due to a scarcity of IP addresses, do not over-estimate the need for addresses. Additional IP ranges can be assigned to an account at a later time.

NOTE! Due to conflicting IP addresses between applications, it is possible that specific IP addresses or ranges of IP addresses cannot be used. Read section 4 before filling in this section of the Product Agreement.

© Copyright Wireless Maingate Nordic AB 2007

Once the customer has sent the completed Product Agreement to Maingate, Maingate will process the agreement and contact the person stated as Technical Contact Person to agree IP addresses and VPN configuration procedures.

When the account has been configured, a confirmation mail with be sent to the Main Contact Person and Technical Contact Person. Attached to the confirmation mail are three documents:

- IP Connect User Guide (this document)
- VPN Configuration Form/ VPN Client, confirming the allocated IP address range and configuration parameters for the VPN tunnel
- IP Connect GPRS Configuration Form, providing login details to the registration API (see section 6), APN (see section 7), IP address to Maingate's NTP server, documentation references on the web and contact details to Maingate Support.

Passwords for the registration API and the VPN pre-shared key or user credentials are sent to the customer in separate emails.

© Copyright Wireless Maingate Nordic AB 2007

4 DEVICE IP RANGES

Since a terminal is identified and addressed using its IP address, it is vital to secure that each terminal always is allocated a unique IP address. IP Connect GPRS performs a check each time a terminal is registered to verify that the IP address is unique.

In order to avoid that different IP Connect GPRS accounts attempt to associate the same IP address to different terminals, each account is only permitted to register IP addresses from a predefined number of IP address ranges. These IP address ranges are compared and verified during product ordering.

NOTE!	If one IP Connect GPRS account has been allocated a certain range of IP addresses, this range cannot be used by another account. This is the reason why Maingate reserves the right to refuse the use of certain IP addresses.

It is possible allocate several IP address ranges to one IP Connect GPRS account.

© Copyright Wireless Maingate Nordic AB 2007

5 IP CONFIGURATION

In order for IP Connect GPRS to function correctly, the transmission of IP packets between Maingate and the customer must be carefully configured. A VPN tunnel is used to carry the traffic between terminals and application. The VPN tunnel ensures that private IP addresses can be used, protects data across the Internet and ensures that one customer's traffic is separated from other traffic.

5.1 VPN CONFIGURATION

IPSec encryption is used for the VPN tunnel between Maingate and the host or LAN connecting the customer application. IPSec is a set of standard protocols for implementing secure communications and encryption key exchange between computers.

An IPSec VPN generally consists of two communications channels between the endpoint hosts: a key-exchange channel over which authentication and encryption key information is passed, and one or more data channels over which private network traffic is carried.

The key-exchange channel is a standard UDP connection to and from port 500. The data channels carrying the traffic between the client and server use IP protocol number 50 (ESP).

More information is available in RFC 2402 (the AH protocol, IP protocol number 51), RFC 2406 (the ESP protocol, IP protocol number 50), and RFC 2408 (the ISAKMP key-exchange protocol).

Configuration details are provided by mail from Maingate after product ordering. The VPN tunnel must be configured according to these methods in order to function.

The IPSec VPN to customer could be set up in two ways. Either with a standard "Site-to-Site" configuration or with a VPN Client software on customer host. Customer will choose which method that is best suitable.

5.2 IP ROUTING

Once the VPN tunnel has been established, the customer LAN or host must be configured to route applicable packets through the VPN and allow packets from the VPN to reach the customer application. When using VPN Client, this would normally been take care off automatically by the software it self.

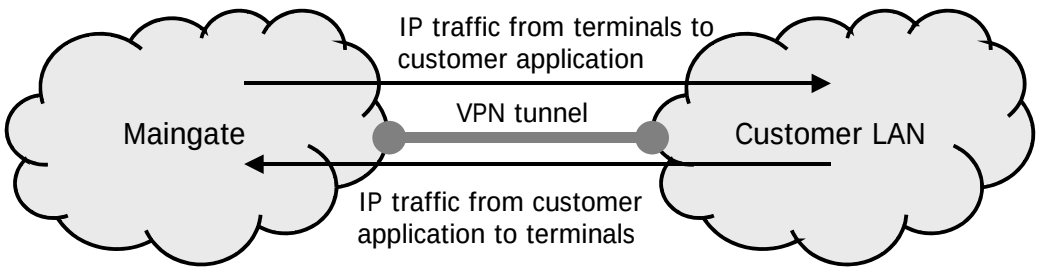


Figure 3 –IP routing between Maingate and customer LAN

The VPN tunnel is only used for data traffic between terminals and application. Transactions to the XML API for registration of terminals shall not be sent though the VPN tunnel. Unencrypted Internet communication is used for transactions towards the XML API, see Figure 4.

© Copyright Wireless Maingate Nordic AB 2007

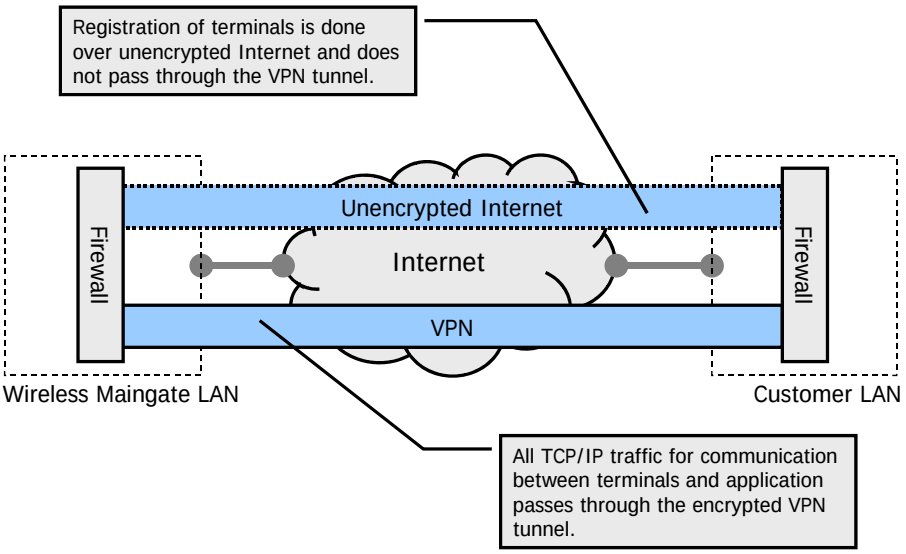

Registration of terminals is done over unencrypted Internet and does not pass through the VPN tunnel.
Unencrypted Internet
Internet
VPN
Firewall
Firewall
Wireless Maingate LAN
Customer LAN
All TCP/IP traffic for communication between terminals and application passes through the encrypted VPN tunnel.

Figure 4 – API transactions over unencrypted Internet, terminal communication through the VPN tunnel.

5.3 FIREWALL CONFIGURATION

The customer must secure that the customer's firewall is open to allow the types of IP sessions to pass that are used by terminal and application. If not, the IP packets will be blocked by the customer's firewall and communication will not function correctly. Wireless Maingate's firewall towards the VPN tunnel is open to allow for all types of IP sessions to pass.

When using VPN Client to access terminals, the firewall protecting the customer host, must be set up to pass through UDP packets bidirectional on port 22022, as the VPN Client recommended by Maingate will use this port to set up the VPN.

5.4 TERMINAL CLIENT CONFIGURATION

IP communication through IP Connect GPRS will not function correctly, if the terminal's IP client is not configured with the correct settings. The terminal must be configured as follows:

- Allow dynamic IP address allocation over PPP
- Default Route or alternatively static routing must be defined for IP Connect GPRS

NOTE!	If dynamic address allocation is not allowed, the terminal will not be able to receive its correct IP address from RADIUS If the Default Route or static routing is not configured, the terminal will be able to connect correctly to IP Connect GPRS, but not be able to communicate with the application.

© Copyright Wireless Maingate Nordic AB 2007

6 REGISTERING TERMINALS

Before communication can take place, every terminal must be registered in Maingate's systems. This is done in one of two ways: Either by using the provided XML API or by sending a list of terminals to be registered to Maingate.

6.1 USING THE XML API

The specification of the XML API is presented in References, [2]. How to use the XML API and general API details can be found in References, [1]. Both documents can be downloaded from: *www.maingate.se/sdk*.

The IP Connect GPRS XML API supports the following calls:

CreateRadiusPost	This call is used to register one or more new terminals.
UpdateRadiusPost	This call is used to modify the parameters of an existing terminal.
DeleteRadiusPost	This call is used to delete an existing terminal from RADIUS.
Export Values	This call is used to generate a file containing the parameter settings of terminals in RADIUS

To register a terminal in RADIUS, the following parameters are used:

MSISDN	This parameter is the mobile number of the terminal. MSISDN must be unique for each terminal.
IP	This parameter is the IP address that is assigned to the terminal from the Device IP Range. IP must be unique for each terminal.

NOTE! The parameters MSISDN and IP must always be unique for each registered terminal.

It may take up to 1 hour after a terminal has been registered or updated in RADIUS before communication is possible to the terminal or the updates take effect.

© Copyright Wireless Maingate Nordic AB 2007

MAINGATE

6.2 MANUAL REGISTRATION USING EXCEL FILE

Instead of using the XML API, the customer may send an Excel file to Maingate that contains a list of terminals to be registered. To initiate a manual registration, the Excel file is sent by e-mail to Maingate's support function. The Excel file must conform to the following specification:

- Clearly identify the customer name, account domain, login and password. These parameters are found in the confirmation mail that the customer has received from Maingate during product ordering (see section 3).
- MSISDN and IP address shall be presented in individual columns, and using one row for each terminal.
- MSISDN shall be presented including country code, without "+" or "00" prefix, and without spaces or symbols to delimit the number, e.g. "46730140102".
- IP address shall be presented with 12 numbers using "0" where necessary and with "." as delimiter, e.g. "100.100.002.009".

NOTE! If the Excel file does not conform to the above description, it will be returned to the customer without being registered.

Should errors occur during registration of terminals from Excel file that are caused by incorrect or conflicting data in the file, the file will be returned to the customer. In this case, data that has been party registered will not be modified in RADIUS.

When the terminals have been successfully registered, Maingate will send a confirmation email to the customer (to the email address that sent the Excel file). After this, the terminals are ready to communicate.

	A	B	C	D	E	F	G
1	**Customer:**	**Test Customer AB**					
2	**IP Connect GPRS Domain:**	**IPCG_test**					
3	**IP Connect GPRS login:**	**testadmin**					
4	**Password:**	**G56hdge%r**					
5							
6	**MSISDN**	**IP**					
7	46710140118	203.012.060.002					
8	46710140119	203.012.060.003					
9	46710140120	203.012.060.004					
10	46710140121	203.012.060.005					
11	46710140122	203.012.060.006					
12	46710140123	203.012.060.007					
13	46710140124	203.012.060.008					
14	46710140125	203.012.060.009					
15	46710140126	203.012.060.010					
16	46710140127	203.012.060.011					
17	46710140128	203.012.060.012					
18	46710140129	203.012.060.013					
19	46710140130	203.012.060.014					
20	46710140131	203.012.060.015					
21	46710140132	203.012.060.016					
22	46710140133	203.012.060.017					
23	46710140134	203.012.060.018					
24	46710140135	203.012.060.019					
25	46710140136	203.012.060.020					

Figure 5 – Example of Excel file structure

© Copyright Wireless Maingate Nordic AB 2007

7 COMMUNICATION

After a terminal has been registered in RADIUS, it is possible to initiate connection to IP Connect GPRS and thereafter communicate to and from that terminal.

7.1 PDP CONTEXT ACTIVATION

Before IP packets can be exchanged between terminal and application, the terminal must connect to IP Connect GPRS. This is accomplished by performing a "PDP Context activation" to the APN provided for IP Connect GPRS from the terminal. (The APN is found in the IP Connect GPRS Configuration Form, see section 3.) The supplier of the GSM modem in the terminal should be consulted regarding how to perform PDP Context activation.

After PDP Context activation has been completed successfully, IP communications can be initiated. Should the PDP Context be lost for any reason, it must be re-activated by the terminal before communication can take place again.

7.2 ADDRESSING TERMINALS

During PDP Context activation, the terminal's IP client will be assigned the IP address that this terminal was assigned during registration (see section 6).

The MSISDN parameter uniquely identifies the terminal and provides the mapping to the correct IP address, which identifies the terminal to the customer application. The mapping of parameters for is shown in Figure 7.

Note!	Even though the terminals use dynamic IP address allocation over PPP, the terminal will always be assigned the same IP address from RADIUS for each PDP Context.

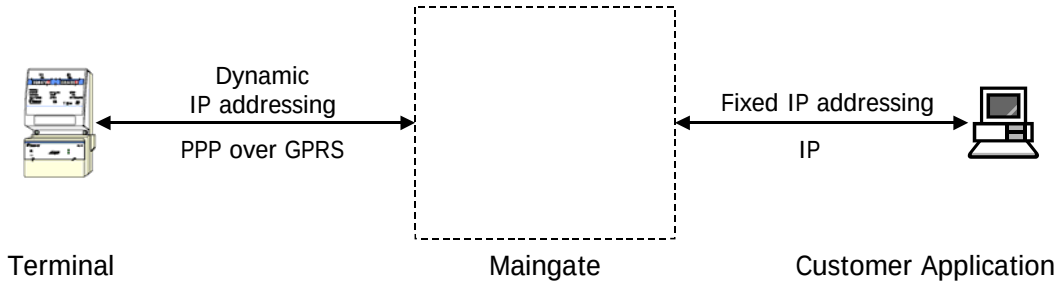


Figure 6 – IP address allocation

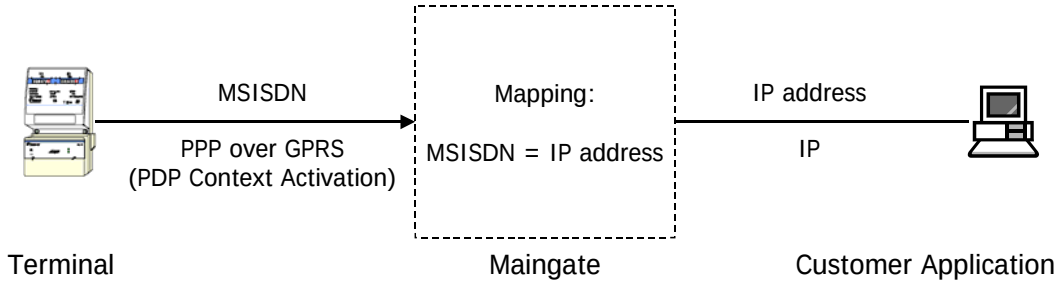


Figure 7 – Parameter mapping during PDP Context activation

© Copyright Wireless Maingate Nordic AB 2007

7.3 DISCONNECTION

Normally, an activated PDP Context does not need to be terminated. The PDP Context can be kept open constantly, to assure that the application can communicate to the terminal. IP Connect GPRS will not initiate a disconnection.

In some cases, the terminal may lose its PDP Context due to network-related issues. Thus, if a constant IP connection to the terminal is required, the terminal must contain functionality to identify a disconnection and automatically reconnect to IP Connect GPRS.

7.4 TIME SYNCRONISATION

Terminals using IP Connect GPRS have access to a local NTP server within Wireless Maingate's LAN. This NTP server can be used to perform time synchronisation of terminals using NTP. The IP-address of Maingate's NTP server is provided in the confirmation mail.

© Copyright Wireless Maingate Nordic AB 2007

8 SECURITY ASPECTS

When using IP-based communication, special attention must always be paid to providing adequate security to protect systems and information. Since use of IP Connect GPRS effectively expands the customer's LAN to a multitude of connection points that potentially can be used by unauthorised persons, special attention to security in this case.

8.1 ACCESSIBLE NETWORK DESTINATIONS

When a terminal is connected via IP Connect GPRS, this terminal can address and communicate with the following network destinations:

1. Customer LAN
2. Maingate's Network Time Server

Figure 8 illustrates the accessible network destinations.

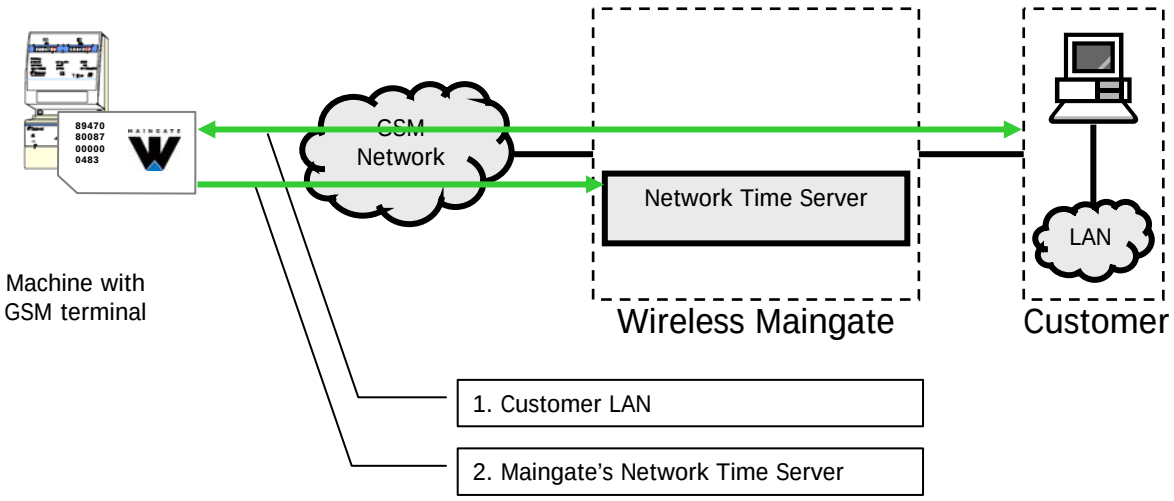


Figure 8 – Accessible network destinations (direction of arrow illustrates what party may initiate communications)

© Copyright Wireless Maingate Nordic AB 2007

8.2 TERMINAL AND APPLICATION SECURITY

Control of a SIM card that is used together with IP Connect GPRS and knowledge of the correct APN, gives a malicious attacker the possibility to address the customer's LAN.

To prevent attacks on the customer's network from a terminal, the customer must use a firewall that blocks malicious IP traffic from reaching his systems.

© Copyright Wireless Maingate Nordic AB 2007

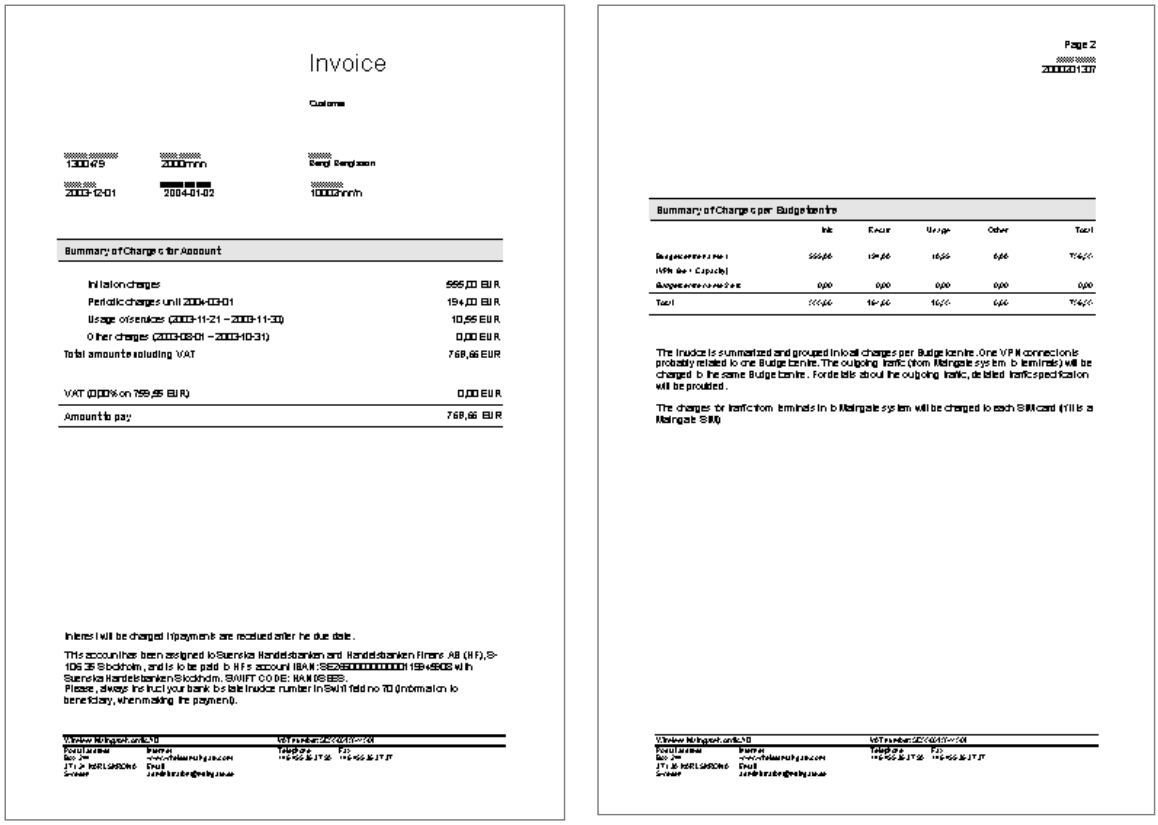
9 INVOICING

Use of IP Connect GPRS is invoiced one time per month. The invoice specifies any applicable initiation fees and periodic fees per account. The structure of fees for IP Connect GPRS is as follows:

Initiation fee	A fixed, one-time fee per account for set-up and configuration of the account
Periodic usage fee	A fixed, yearly fee per account for use of IP Connect GPRS
Periodic capacity fee	A variable, monthly fee per account that depends on the number of subscriptions that are registered for use through that account
Registration fee	A fixed fee per Excel file that has been registered by Maingate

Note! All GPRS traffic between terminal and application through IP Connect GPRS are invoiced to the respective subscription that has initiated the PDP Context.

An example of an invoice is shown in Figure 9.


Invoice

Customer

Summary of Charges for Account

Initiation charges	555,00 EUR
Periodic charges until 2004-03-01	194,00 EUR
Usage of services (2003-11-21 – 2003-11-30)	10,66 EUR
Other charges (2003-03-01 – 2003-10-31)	0,00 EUR
Total amount excluding VAT	768,66 EUR
VAT (0,00% on 768,66 EUR)	0,00 EUR
Amount to pay	768,66 EUR

Interest will be charged if payments are received after the due date.

This account has been assigned to Svenska Handelsbanken and Handelsbanken Finans AB (HFA), S-106 35 Stockholm, and is to be paid to HFA's account IBAN: SE2650000000001594568 with Svenska Handelsbanken Stockholm, SWIFT CODE: HANDSESS.
Please, always instruct your bank to state invoice number in SWIFT field no 70 (information to beneficiary, when making the payment).

Page 2

Summary of Charges per Budget Centre

	Init	Fixed	Usage	Other	Total
Budget centre 1 Part 1	555,00	194,00	10,66	0,00	759,66
VPN Geo Capacity					
Budget centre 1 Part 2	0,00	0,00	0,00	0,00	0,00
Total	555,00	194,00	10,66	0,00	759,66

The invoice is summarized and grouped in local charges per Budget centre. One VPN connection is probably related to one Budget centre. The outgoing traffic (from Maingate system to terminals) will be charged to the same Budget centre. For details about the outgoing traffic, detailed traffic specification will be provided.

The charges for traffic from terminals in to Maingate system will be charged to each SIM card (YTI is a Maingate SIM)

Figure 9 – Example of invoice

© Copyright Wireless Maingate Nordic AB 2007

10 SUPPORT

IP Connect GPRS customers are automatically entitled to the use of Maingate Support. Maingate Support is staffed by qualified personnel that have thorough experience in supporting customers using GSM communication for industrial applications.

The support organization helps customers with the following queries:

- Administration of subscriptions and SIM cards
- Invoicing queries
- Ordering and managing Maingate's products
- Troubleshooting
- Queries about technical product functions
- Information about planned outages and operational disturbances

Maingate Support can be reached via telephone, fax or e-mail. Contact details are supplied with the product confirmation e-mails that are sent to customers after product ordering.

More information regarding Maingate support is presented in reference [3].

© Copyright Wireless Maingate Nordic AB 2007

11 REFERENCES

[1] Interface Specification HTTP/XML, MG000137 AU, revision D
[2] IP Connect GPRS Interface Specification, MG040116 AU, revision A
[3] Service Level Agreement, MG020973 PdM, revision B

12 DOCUMENT HISTORY

Revision	Date	Signature	Comments
A	2004-11-02	Niklas E	First sharp revision
B	2004-11-22	Niklas E	Modification section 2.2 and 3
C	2005-04-29	Niklas E	
D	2005-11-14	Niklas E	Modifications section 4 and 9
E	2006-10-20	Helén S	Modifications section 8 and 10
F	2007-10-03	HS, TS	Added VPN Client

© Copyright Wireless Maingate Nordic AB 2007